Sub A1

CLAIMS

1. A method for detecting within a networked computer a target vulnerability residing therein, the vulnerability being characterized by a signature response to an encrypted query, the method comprising:

encrypting a query data packet in accordance with a plurality of encryption keys to produce a plurality of encrypted query data packets, each encrypted query data packet including a defined query field specific to the target vulnerability;

storing the plurality of encrypted query data packets in a memory; and thereafter

scanning the networked computer for a target vulnerability residing therein by sending successive ones of the encrypted-and-stored query data packets to the networked computer and analyzing responses thereto from the networked computer with respect to the characteristic signature.

2. The method of claim 1 in which plural networked computers are so scanned by sending the encrypted-and-stored query data packets to each of plural networked computers and by analyzing responses thereto from each of the plural networked computers.

3. The method of claim 1 in which plural ports of plural networked computers are so scanned by sending the encrypted-and-stored query data packets to each of plural ports of each of plural networked computers and by analyzing responses thereto from each of the plural ports of each of the plural networked computers.

4. The method of claim 1 wherein the target vulnerability is Trojan Horse software residing in a port of the networked computer.

5. The method of claim 4 wherein the encrypted data packet includes an encrypted command field recognizable by the Trojan Horse software.

6. The method of claim 1 wherein said encrypting is performed for substantially all of the encryption keys within a defined key space.

7. The method of claim 1 wherein said storing is to a non-volatile memory.

8. The method of claim 7 which further comprises writing the stored plurality of encrypted query data packets from the non-volatile memory to a cache memory prior to said scanning.

9. Apparatus for detecting one or more Trojan Horses resident within one or more computers connected with a network, the apparatus comprising:

a pre-processor for encrypting a query data packet in accordance with a plurality of different keys and storing a plurality of such differently encrypted query data packets in a database, the query data packet including one or more fields of data to which a Trojan Horse if resident in a given computer would make a signature response;

a memory device for storing the database;

a transmitter for transmitting said database to a plurality of computers connected with a network; and

an analyzer for analyzing responses from the plurality of computers to said transmitting, said analyzer recognizing and recording one or more signature responses along with one or more corresponding addresses of the one or more signature-respondent computers.

10. The apparatus of claim 9 wherein said memory device is non-volatile.

11. The apparatus of claim 9 wherein said memory device is a random-access memory (RAM).

12. The apparatus of claim 9 wherein said memory device is organized as a cache.

13. The apparatus of claim 9 wherein said different keys include substantially all keys in a given key space.

14. A computer-readable medium containing a program for detecting within a networked computer a target vulnerability residing therein, the vulnerability being characterized by a signature response to an encrypted query, the program operable to perform the following steps:

encrypting a query data packets in accordance with a plurality of encryption keys to produce a plurality of encrypted query data packets, each encrypted query data packet including a defined query field specific to the target vulnerability;

storing the plurality of encrypted query data packets in a memory; and

scanning the networked computer for a target vulnerability residing therein by transmitting successive ones of the encrypted-and-stored query data packets to the networked computer and analyzing responses thereto from the networked computer with respect to the characteristic signature.

15. The program of claim 14 wherein said storing is in a non-volatile memory.

16. The program of claim 14 wherein said storing is in a random-access memory (RAM).

17. The program of claim 14 wherein said storing is in a memory configured as a cache.

18. The program of claim 14 wherein said plurality of encryption keys number at least a substantial fraction of a given key space.

19. The program of claim 18, wherein said plurality of encryption keys represent substantially all keys in the given key space.